DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF

REAR ADMIRAL CRAIG BONE
DIRECTOR OF INSPECTION AND COMPLIANCE
U.S. COAST GUARD

MARK HATFIELD
DEPUTY FEDERAL SECURITY DIRECTOR
FOR NEWARK LIBERTY INTERNATIONAL AIRPORT
TRANSPORTATION SECURITY ADMINISTRATION

ON THE

NATIONAL STRATEGY FOR MARITIME SECURITY

BEFORE THE

COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE

SUBCOMMITEE ON COAST GUARD AND MARITIME TRANSPORTATION

U. S. HOUSE OF REPRESENTATIVES

JANUARY 24, 2006

Good afternoon Mr. Chairman and distinguished Members of the Committee. It is our pleasure to be here today to testify on the National Strategy for Maritime Security.

An Overview of National Strategy for Maritime Security

On December 21, 2004, President Bush signed National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD-41/HSPD-13) with the goal of establishing U.S. policy, guidelines, and implementation actions to enhance U.S. national security and homeland security. It directs that all U.S. Government maritime security programs and initiatives be coordinated in order to achieve a comprehensive and cohesive national effort involving appropriate federal, state, local and private sector entities. The Secretaries of Defense and Homeland Security were jointly charged with leading a collaborative interagency effort to craft a National Strategy for Maritime Security (NSMS) and eight supporting plans. The NSMS highlights some key ideas:

- The safety and economic security of the United States depend upon the secure use of the world's oceans. Maritime security harmonizes the need for protection against terrorist, hostile, criminal and dangerous acts with the need for vibrant, secure maritime commerce that underpins economic security and well-being. Therefore, the United States has a vital national interest in maritime security.
- Maritime domain security is a global issue. Because all nations benefit from this collective security, all nations must share in the responsibility for maintaining maritime security;
- Security in the maritime domain is a shared responsibility between the public and the private sectors.
- Maritime security encompasses threats from all criminal or hostile acts, such as the smuggling of contraband, illegal immigration, piracy, illegal harvesting of natural resources, and the threat of terrorist activities.

The NSMS strives for a holistic approach to dealing with the broad array of threats, addressing activities that span from prevention to post-incident recovery to achieve the following four objectives:

- Prevent successful terrorist attacks and criminal or hostile acts;
- Protect maritime-related population centers and critical infrastructure;
- Minimize damage and expedite recovery; and
- Safeguard the ocean and its resources.

The National Strategy strives to achieve its objectives through five cross-cutting strategic actions:

- Enhance international cooperation to ensure lawful and timely actions against maritime threats;
- Maximize domain awareness to support effective decision-making;
- Embed security into commercial practices to reduce vulnerabilities;
- Deploy layered security to unify public and private security measures; and
- Assure continuity of the marine transportation system to maintain vital commerce.

U.S. COAST GUARD

Implementing the National Strategy

NSPD-41/HSPD-13 created an interagency Maritime Security Policy Coordinating Committee (MSPCC) to serve as the primary forum for coordinating U.S. Government maritime security policies. The MSPCC coordinated the development of the NSMS and its supporting plans, and is now actively working on assigning responsibilities and tasks to agencies within the government for implementation.

Maritime Operational Threat Response or MOTR

The Maritime Operational Threat Response, or "MOTR" Plan, is part of the President's National Strategy for Maritime Security. In 2005, as part of the National Strategy for Maritime Security, Department of Homeland Security (DHS), Department of Justice (DOJ), and the Department of Defense (DOD) developed the MOTR Plan, which builds upon and improves the PD-27 process to ensure nationally coordinated maritime operational response to address the full spectrum of 21st Century maritime security and defense threats to, or directed against, the United States and its interests globally. MOTR addresses the full range of maritime security threats, including actionable knowledge of or acts of terrorism, piracy and other criminal or unlawful or hostile acts committed by both state and non-state actors. Maritime operational threat response includes the deployment of capabilities and use of force required to intercept, apprehend, exploit, and when necessary, defeat maritime threats. Implementation of the MOTR Plan envisions employing an integrated network of existing national-level maritime command and operations centers to achieve coordinated, unified, timely and effective planning and mission accomplishment by the U.S. Government. The MOTR Plan establishes the protocols and procedures for achieving that coordinated response and ensuring the delivery of desired U.S. outcomes. MOTR provides an effective mechanism for the United States to approach maritime security threats and to develop timely and tailored responses based on dispersed authorities, capabilities, competencies and partnerships. In short, MOTR improves the ability of the United States to bring the right assets to bear when maritime threats affect American interests anywhere in the world.

Integrating the Layers of Security

The concept of "layers of security" is complex, involving multiple types of activities to create a network of interdependent, overlapping and purposely redundant checkpoints designed to reduce vulnerabilities, as well as detect, deter and defeat threats. It entails developing security measures that cover the various components of the maritime transportation system, including people, infrastructure, conveyances and information systems. These security measures span distances geographically—from foreign ports of embarkation, through transit zones, to U.S. ports of entry and beyond—and involve the different modes of transportation that feed the global supply chain; and are implemented by various commercial, regulatory, law enforcement, intelligence, diplomatic and military entities. A significant challenge to constructing integrated layers of security is the fact that many of the layers are the responsibility of different agencies. Integrating these disparate maritime security layers involves not only unity of effort, shared responsibility, partnership, and mutual support, but requires an agency with significant maritime security responsibilities to step up and act as a coordinator for the purposes of integrating the government's efforts to provide layered security.

Developing Maritime Domain Awareness

The National Strategy for Maritime Security defines Maritime Domain Awareness (MDA) as "the effective understanding of anything associated with the global Maritime Domain that could impact the security, safety, economy or environment of the U.S." MDA is neither a program nor a mission, but rather a state of awareness necessary to achieve maritime security. DHS therefore has tasked the Coast Guard to act on its behalf for implementing the systems and processes necessary to achieve the level of MDA required by the National Strategy. The MDA Implementation Team, co-led by DOD and the Coast Guard, oversees the implementation of the National Plan to Achieve MDA. This plan is a cornerstone for the successful execution of the National Strategy for Maritime Security and serves to unify efforts across the Federal Government, with the private sector and civil authorities within the United States, as well as, with our allies and international partners. MDA has many stakeholders. Within DHS, it supports and is supported by U.S. Customs and Border Protection (CBP), the Coast Guard, U.S. Immigration and Customs Enforcement (ICE), and the Transportation Security Administration (TSA). MDA also supports and is supported by DOD, as well as DOJ and other federal, state and local law enforcement agencies.

Preparing for Maritime Recovery Operations

The private sector has traditionally demonstrated an ability to adjust their activities in response to disruptions in the maritime transportation system, so much so that it has often been said to be "self-healing" in nature. Widespread disruptions caused by a security-related incident of national significance, however, could threaten to bring large portions of the maritime transportation system to a virtual standstill; hence, contingencies must be prepared. Assuring continuity of commerce requires extensive coordination between the public and private sectors in order to restart or keep the flow of commerce moving during or following such an event. On the national level, recovery policies and procedures that emphasize assuring continuity of commerce in the maritime domain, such as the Maritime Infrastructure Recovery Plan and the Plan to Re-establish Cargo Flow, must be closely coordinated with the other federal agencies and, most critically, the private sector.

Partnering for International Maritime Diplomacy

The Coast Guard, in consultation with the Department of State, the lead agency for international affairs, now more than ever, will play a vital role as an instrument of national security in protecting, promoting and defending the maritime interests of the United States and our international partners around the world. In our international maritime diplomacy role, the Coast Guard can assist other nations in: (1) development of national maritime policies, strategies, standards and legislation; (2) the professional and material development of national maritime security, maritime safety and naval forces; and (3) the development of other maritime management and regulatory regimes. The Coast Guard has traditionally been the chief advocate for the United States in international issues involving maritime safety. Since 2001, the Coast Guard has led interagency efforts to establish a maritime security regime via international forums such as the International Maritime Organization (IMO).

International Port Security Assessments

Internationally, we continue our efforts visiting foreign countries to assess the effectiveness of anti-terrorism measures in foreign ports. To date, 43 countries have been assessed, with China being the most recent visit, and 35 have been found to be in substantial compliance with the ISPS. The Coast Guard is on track to assess approximately 45 countries per year and our goal remains to visit about 140 countries with whom we trade by September 2008.

Long Range Identification and Tracking (LRIT)

Long Range Identification and Tracking (LRIT) is another area we have been pursuing on an international front. LRIT is all about increasing the transparency of vessels plying the global maritime concourse. It provides for persistent detection, classification, identification and tracking of cooperative vessels. This capability will align decision makers and operational commanders so they have a clearer understanding of the vessel traffic in areas of interest.

Through the International Maritime Organization, we, collectively, have taken the first step in making LRIT a reality – drafting amendments to the 1974 SOLAS Convention that address the interests of all countries concerned. It is also important to note that the proposed text of the LRIT amendment will make it clear that possession of LRIT information, by itself, gives Contracting Governments no new authority to act. Rather, it gives them the ability to acquire information on the whereabouts of vessels of concern to them.

Maritime and Cargo Security

The Coast Guard works in concert with CBP to align respective agency roles and responsibilities regarding international trade. When cargo is moved on the waterborne leg of a trade route, the Coast Guard has oversight of the cargo's care and carriage on the vessels and within the port facility. The Coast Guard also oversees the training and identity verification of the people who are moving the cargo. CBP has authority over the cargo contents and container standards. Using the information

provided through the Coast Guard's 96-hour notice of arrival rule and CBP's 24-Hour cargo loading rule, the Coast Guard and CBP act to control vessels (and their cargoes) that pose an unacceptable risk to our ports. As a further improvement, the trade community can file required passenger and crew information via an electronic notice of arrival and departure system. This streamlines the process for industry and improves our ability to apply targeting and selectivity methods. With Coast Guard officers posted at the NTC, we continuously improve agency coordination and our collective ability to quickly take appropriate action when notified of a cargo of interest.

Additionally, DHS has worked hard to align all of our regulatory and policy development efforts with CBP, the Coast Guard, and TSA. We meet regularly to discuss policy, participate on inter-agency regulation development teams and sit on the Operation Safe Commerce Executive Steering Committee. Between DHS, CBP and the Coast Guard, we coordinate the work of our various Federal Advisory Committees so that we all understand the trade community's concerns and priorities. Now that Maritime Transportation Security Act of 2002 and the International Ship and Port Facility Security (ISPS) Code have been implemented at the port, facility and vessel levels, we are monitoring compliance and carefully noting issues for future improvements to the regulatory framework.

U.S. CUSTOMS AND BORDER PROTECTION

CBP plays a significant role in maritime security and cargo security for the Department. CBP, as the guardian of the Nation's borders, safeguards the homeland---foremost, by preventing the entry of terrorists and instruments of terror into the United States, while, at the same time, enforcing the laws of the United States and fostering the Nation's economic security through lawful travel and trade. Contributing to all this is CBP's time-honored duty of apprehending individuals attempting to enter the United States illegally, stemming the flow of illegal drugs and other contraband, protecting our agricultural and economic interests from harmful pests and diseases, protecting American businesses from theft of their intellectual property, regulating and facilitating international trade, collecting import duties and enforcing U.S. trade laws.

In the aftermath of the terrorist attacks of September 11, 2001, the legacy U.S. Customs Service (now CBP) developed initiatives to meet our twin goals of improving security and facilitating the flow of legitimate trade and travel. CBP's homeland defense strategy to secure and facilitate cargo moving to the United States is a layered defense approach built upon five (5) interrelated initiatives. These initiatives include: the 24-Hour Rule and Trade Act rules, the Automated Targeting System (ATS) (housed in CBP's National Targeting Center (NTC)), the wide-spread use of sophisticated non-intrusive inspection (NII) technology at ports of entry, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT).

Advance Electronic Information

As a result of the 24-Hour Rule and the Trade Act, CBP requires advance electronic information on all cargo shipments coming to the United States by land, air and sea, so that we know who and what is coming before it arrives in the United States.

Automated Targeting System

The Automated Targeting System is essential to CBP's ability to target high-risk cargo and passengers entering the United States. ATS is the system through which we process advance manifest and passenger information to detect anomalies and "red flags" and determine which passengers and cargo are "high risk" and should accordingly be scrutinized at the port of entry or, in some cases, overseas.

ATS is a flexible, constantly evolving system that integrates enforcement and commercial databases. ATS analyzes electronic data related to individual shipments prior to arrival and ranks them in order of risk based on the application of algorithms and rules. The scores are divided into thresholds associated with further action by CBP, such as document review and inspection.

Detection Technology at Air, Land and Sea Ports of Entry

NII technologies, including radiation detection equipment, are a critically important component of CBP's layered enforcement process that enable us to screen a larger portion of the stream of commercial traffic in less time while facilitating legitimate trade. Since September 11, 2001, CBP has developed a multi-faceted strategic approach to address the radiological smuggling threat that begins outside of the United States where the movement of nuclear and radiological materials may be initiated, and continues to the U.S. border. We currently have 170 large-scale NII imaging systems deployed (including 59 systems to seaports), 567 radiation portal monitors (RPMs) deployed (including 143 RPMs to seaports), 549 radiation isotope identification devices (RIIDs) deployed (including 200 RIIDs to seaports), and 12,449 personal radiation devices (PRDs) deployed (over 3,500 PRDs to seaports). Used in combination with our layered enforcement strategy, these tools provide CBP with a significant capability to detect nuclear or radiological materials.

Container Security Initiative

Every day, approximately 25,000 seagoing containers arrive at the Nation's seaports equating to nearly 9.2 million a year. About 90% of the world's manufactured goods move by container, much of it stacked many stories high on huge transport ships. Each year, 200 million cargo containers are transported between the world's seaports, constituting a critical component of global trade.

The fact is that, today, the greatest threat we face to global maritime security is the potential for terrorists to use the international maritime system to smuggle terrorist weapons – or even terrorist operatives – into a targeted country.

Clearly, the risk to international maritime cargo demands a robust security strategy that can identify, prevent and deter threats at the earliest point in the international supply chain, before arrival at a seaport of a targeted country. The Nation developed a cargo security strategy that addresses cargo moving from areas outside of the United States to our ports of entry. Our strategy focuses on stopping any terrorist shipment before it reaches the United States and then, only as a last resort, at a U.S. port of entry, if it should arrive there.

CSI enables CBP to work with our host counterparts to screen and inspect high-risk containers before they are loaded on board vessels to the United States. CBP implemented CSI in January 2002 because we recognized that inspecting containers with terrorist weapons concealed inside them, on arrival in the United States, would be too late. Today, CSI is one of the few multinational programs in the world actually protecting the primary means of global trade – containerized shipping – from being exploited or disrupted by international terrorists.

Through the CSI program, CBP deploys multi-disciplined teams comprised of agents, intelligence analysts, and CBP officers to selected foreign seaports throughout the world, to protect the United States and its citizens from both direct and indirect terrorist attacks in the maritime cargo environment. A critical component of the CSI program is the Non-Intrusive Inspection (NII) equipment, which includes radiation detection equipment, that allows the CBP teams sent to foreign ports to select containers for inspection prior to placement of the container on a ship bound for the United States, based on established risk factors and current intelligence. Under the CSI program, CBP may also loan foreign authorities non-intrusive inspection and radiation detection equipment until such time as the foreign authority is able to procure its own equipment, and CBP may provide

training for domestic or foreign personnel involved in the CSI program. Today, CSI is operational in 42 ports in Europe, Asia, Africa, North America, and South America. CBP is working towards strategically locating CSI in additional foreign seaports with a nexus to terrorism.

To inspect all high-risk containers before they are loaded on board vessels to the United States, CBP plans to continue fostering partnerships with other countries and our trading partners. In addition, the World Customs Organization, the European Union and the G8 support CSI expansion and have adopted resolutions implementing CSI security measures introduced at ports throughout the world.

Customs-Trade Partnership Against Terrorism (C-TPAT)

The Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary partnership between CBP and industry to secure the international supply chain. C-TPAT importers secure supply chains from the foreign factory loading docks of their vendors to the port of arrival in the United States. CBP, in return, offers C-TPAT shipments expedited processing and provides C-TPAT participants with other benefits.

To join C-TPAT, a company must conduct a comprehensive self-assessment of its current supply chain security procedures using C-TPAT security criteria and best practices developed in partnership with the trade. A participant must also commit to increasing its supply chain security to meet minimal supply chain security criteria. Perhaps most importantly, participants also make a commitment to work with their business partners and customers throughout their supply chains to ensure that those businesses also increase their supply chain security. By leveraging the influence of importers, C-TPAT is able to increase security of U.S-bound goods to the point of origin (i.e., to the point of container stuffing). This reach – to the foreign loading dock – is beyond the regulatory reach of the U.S. Government, but critical to the goal of increasing supply chain security.

C-TPAT is currently open to all importers, cross-border air, sea, truck, and rail carriers, brokers, freight forwarders, consolidators, non-vessel operating common carriers, and U.S. Marine and Terminal operators. We are currently enrolling certain foreign manufacturers in the C-TPAT program and will continue to develop ways to include this important element of the supply chain in the program. The intent is to increase point of origin to point of arrival security into the supply chain.

Although C-TPAT is a partnership, the risk is too great to simply take participants at their word when it comes to their supply chain security. We have created a cadre of specially trained supply chain security specialists to validate the commitments made by C-TPAT participants and to ensure that the participants are increasing supply chain security as they have promised and that their measures are reliable and effective. These specialists meet with personnel from C-TPAT certified companies and their business partners and observe the security of their supply chains, including security at overseas loading docks and manufacturing plants, as well as transportation links outbound to the United States. Through this validation process, we work with certified members to identify ways that they can further increase their supply chain security. Companies that are not honoring their commitments may be suspended or removed from the program and lose their C-TPAT benefits.

As of January 6, 2006, C-TPAT has assessed and accepted the security profiles of 5,651 companies; there are more than 4,700 company profiles in various stages of the application and review process. We have completed 1, 480 validations, with an additional 2,304 validations underway or in the process of being completed.

Automated Commercial Environment (ACE) and the International Trade Data System (ITDS)

CBP has also worked vigorously to continue expansion of its Automated Commercial Environment (ACE), a multi-year modernization effort to reengineer critical business processes with the trade community and the information technology that supports them. This effort will greatly assist CBP in the advance collection of information for targeting high-risk cargo to better address terrorist threats and other high security concerns. And in doing so, it will help us expedite the vast majority of low-risk trade.

One important, fully integrated component of ACE is the International Trade Data System (ITDS). The ITDS initiative is an e-Government strategy being designed developed, and deployed jointly with ACE that will implement an integrated, government-wide system for the electronic collection, use, and dissemination of the international trade transaction data required by various trade-related federal agencies.

ITDS simplifies and streamlines the regulation, promotion, and analysis of international trade. It assists importers, exporters, carriers, and brokers in complying with federal trade, transportation, and other regulations by streamlining business processes. ITDS is customer focused and will serve as the government's 'single window' into international trade data collection and distribution.

In conjunction with ACE, ITDS will also improve risk assessment. By centralizing and integrating the collection and analysis of information, ACE will enhance CBP's ability to target cargo, persons, and conveyances. The trade data will allow for advanced inter-agency assessment of risks and threats to determine which goods and people must be scrutinized. In addition, through ACE, the ITDS will be capable of linking the government's law enforcement and other databases into one large-scale relational database that tracks all commerce crossing our borders. ITDS thus extends the functionality of ACE by bringing together critical security, public health, public safety, and environmental protection agencies under a common platform.

TRANSPORTATION SECURITY ADMINISTRATION

PortSTEP

Intermodal transportation systems converging at America's ports are highly interdependent and of great economic importance. Consequently, these networks have a high criticality rating and demand significant security attention. TSA and the Coast Guard have jointly developed and implemented the Port Security Training Exercises Program (PortSTEP), which contribute to meeting the mandates of the 2002 Maritime Transportation Security Act. PortSTEP is designed to provide maritime transportation security communities nationwide with training exercises, evaluations and accompanying information technology products to help strengthen the Nation's ability to prevent, respond to, and recover from a transportation security incident (TSI) in a port and maritime environment.

The first PortSTEP exercise occurred in San Francisco in August 2005. Seven more occurred during the balance of the year in Baltimore, Maryland; Anchorage, Alaska; Boston, Massachusetts; Puget Sound, Washington; Corpus Christi, Texas; Tampa, Florida; and Duluth, Minnesota. Valuable lessons have been learned and applied to improve intelligence information sharing, communications procedures, training programs and Area Maritime Security planning. Each PortSTEP exercise builds on the experience previously gained in a continual effort to deliver a top quality product and maximize its value in enhancing security of ports and intermodal systems. A total of 17 exercises are scheduled for 2006, building toward the objective of conducting 40 exercises in all. PortSTEP development will end in October 2007, culminating in a fully vetted and tested port and

transportation security exercise pilot program that can serve as a model for TSA and other government agencies.

Delivered through the Area Maritime Security Committees (AMSCs), PortSTEP fosters and supports institutional relationships within the port environment including federal, state and local government partners, the surface transportation industry, intermodal transportation security managers, emergency managers, law enforcement, medical professionals, media, security personnel and all others involved in preparing for and responding to a TSI.

Secure Automated Inspection Lanes (SAIL) Program.
In coordination with the Coast Guard, TSA has implemented the SAIL test project to develop screening technologies and capabilities aimed at enhancing security on ferry systems. This multi-phased effort has tested and evaluated the use of explosives detection systems on two major ferry systems. TSA deployed a van portable Z backscatter X-ray system on the Cape May-Lewes Ferry, which carries vehicles and passengers between the southern tip of New Jersey and Delaware, and explosives detection document scanners on the high volume passenger-only commuter ferry in San Francisco Bay. Planning is under way to initiate a third phase, which will test a total screening program for both passengers and vehicles in a large commuter ferry operation.

Security Screening Research and Development.
TSA is managing a $3.69 million research and development grant program to test and evaluate explosive trace detection equipment for screening passengers, baggage and vehicles in the ferry and cruise line industries. A request for applications for grant awards for vehicle screening equipment will be published this spring. Grants for passenger and baggage screening equipment have already been awarded, and procurement of that equipment for testing by the Transportation Security Laboratory in Atlantic City is underway. After completion of a 30-day test period, deployment of equipment will commence for field tests across the maritime passenger industry.

Miami Synergy Project.
TSA operates the Miami synergy project, a joint baggage screening initiative targeting the intermodal junction of passengers changing between cruise ships and commercial air travel. In this program, baggage from Royal Caribbean Cruise Lines passengers is screened at the seaport by TSA personnel using portable machines and then transferred in-bond to American Airlines flights operating out of Miami International Airport. The program has significantly reduced congestion and stress on TSA screeners at the airport and received highly positive reviews from passengers. The Miami seaport baggage-screening program has averaged 1000 passengers and 1500 pieces of check-in luggage per 3 days of operation each week. To date, 112,842 passengers and 158,528 pieces of baggage have undergone security screening in this initiative.

Transportation Worker Identification Credential (TWIC)
The TWIC program was initiated by TSA in its earliest days to ensure that only properly cleared and authorized personnel could gain access to secure areas of the Nation's transportation system.

The goals of the TWIC program are to:

- Develop a common, secure biometric credential and standards that are interoperable across transportation modes and compatible with existing independent access control systems;
- Establish processes to verify the identity of each TWIC applicant, complete a security threat assessment on the identified applicant, and positively link the issued credential to that applicant; and

- Quickly revoke card holder privileges for individuals who are issued a TWIC but are subsequently determined to pose a threat after issuance of their credentials, and immediately remove lost, stolen, or compromised cards from the system.

TSA developed a plan to build the TWIC program in four phases: Phase I - Planning, Phase II - Technical Evaluation, Phase III - Prototype, and Phase IV - Implementation. TSA recently completed executing Phase III – Prototype testing, in which the overall TWIC solution was evaluated against a full range of business processes, policies and requirements, including enrollment centers and enrollment, security threat assessments, verification of claimed identity, card personalization and production, card issuance and revocation.

Encompassed within the TWIC program are requirements established by the Maritime Transportation Security Act of 2002 (MTSA), Pub. L. No. 107-295, to prevent unaccompanied individuals from entering a secure area of a vessel or facility unless the individual holds a transportation security card. Additionally, the Act requires that all holders of Merchant Mariner Credentials obtain a TWIC. With MTSA as their guide, the Coast Guard and TSA have worked closely to develop the maritime component of TWIC and are currently preparing a joint Notice of Proposed Rulemaking (NPRM).

Full implementation of TWIC requires promulgation of a rule establishing standards for security threat assessments of workers with unescorted access to secure areas of maritime facilities and vessels, a biometric identification credential that reflects the results of a satisfactory assessment, access control procedures to prevent unauthorized entry into secure areas and redress for workers who are denied a TWIC. Issuance of the rule will also implement the fee authority enabling the program to be fully supported through user fees. TSA and the Coast Guard are utilizing the experience and information gained through Phase III-Prototype testing of the project, in which various access control systems were established, security threat assessments were conducted and biometric credentials were issued.. The Prototype testing phase was completed in the summer of 2005, paving the way for TSA and the Coast Guard to move ahead with the rule.

The initial rollout of TWIC in the maritime arena will impact port workers, merchant mariners and personnel in the trucking and rail modes who require unescorted access to port facilities and vessels.

In the NPRM, TSA and USCG will address statutory requirements that card production take place at a centralized, highly secure federally managed card production facility. Once produced, cards will be sent via express delivery services to the enrollment center where the applicant enrolled. The finished card will be issued at the enrollment center once the applicant has matched their biometric to the card. At that time the card will be activated and ready for use in the TWIC system.

The Coast Guard is working very closely with the TSA to assist in the implementation of this new credentialing program. The Coast Guard is supportive of this regulatory effort. We will do everything within our ability to assist TSA in the development of this rulemaking and ensure that the TWIC and Merchant Mariner Credentialing initiatives are complementary in order to minimize the burden on mariners in the future.

Maritime Cargo Container Security Initiatives.

TSA has provided dedicated support and has substantially contributed to the development of several programs to enhance security of maritime cargo containers.

- TSA is exploring programs to enhance cargo security across the maritime and intermodal transportation system.

- Through Operation Safe Commerce, originally a TSA initiative now led by the Department's Office of Domestic Preparedness, development projects aim to increase security throughout the foreign and domestic supply chain through the use of container seal devices and other technologies. The program is now completing Phase III and product testing.

- From February 28 to March 2, 2006, TSA will jointly host with DOD the biennial Security Seals Symposium. This event, a continuing program now in its seventh iteration, provides a forum for exchange of information and technology between government and the maritime industry. The Symposium will explore operational, procedural, and technical issues affecting security seals, tamper-indicating devices, and radio frequency identification (RFID) technology. Speakers and panel discussions will cover a broad range of subjects, including protection of cargo shipments into and within the United States, the role of security seals and associated products in meeting changing and challenging security requirements, international coordination to develop security seal requirements and standards to protect assets in transit and container monitoring and cargo transportation security and integration of technology.

Summary

Over the past several months and years, each of these efforts has begun to help us further the goals of the National Strategy for Maritime Security and will now be approached from the framework of that strategy and its supporting plans.

While the National Strategy for Maritime Security's primary focus is on securing the Nation's ports, waterways and coastal approaches, the funding provided for maritime security has enhanced our ability to increase awareness, outreach, prevention, response and recovery capabilities. The events of September 11, 2001, heavily influenced our focus on security, but natural disasters such as Hurricanes Katrina and Rita remind us of other vulnerabilities and threats to the Nation.

As stated in the NSMS, it is only through an integrated approach among all maritime partners—domestic and international, public and private—that the security of the maritime domain can successfully be improved. Such collaboration is fundamental to implementing this National Strategy and vital to protecting the interests of the United States.

Thank you for your time and we will be happy to answer any questions you may have.